

Intelligence Writing - Why It Matters

Table of Contents

Intelligence Writing – Why It Matters	2
Why Intelligence Writing Matters	3
Intelligence Writing – Some Tips	4
Know your Audience	6
Intelligence Writing Is Not Academic Writing -1	7
Intelligence Writing Is Not Academic Writing -2	8
Bottom-Line-Up-Front (BLUF)	10
BLUF 1st Paragraph Tips	11
Key Judgements	12
Source Summary Statement	13
Intelligence Gaps.....	15
Threat and Strategic Analysis.....	16
Conclusion	17
Intelligence Writing Tips -1	19
Intelligence Writing Tips -2	20
Intelligence Writing Tips -3	21
Notices	22

Intelligence Writing – Why It Matters

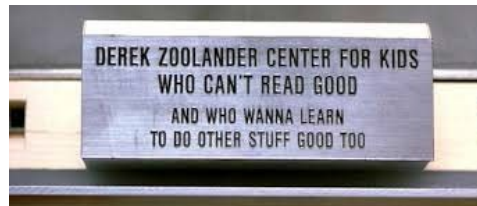


Intelligence Writing – Why It Matters

39

**039 Let's talk about intelligence writing and why it matters.

Why Intelligence Writing Matters



“If you are not able to clearly communicate the results of all the research, analysis, and other grunt work you have put in, then, from the reader’s viewpoint, none of that mattered.”

- Writing and Briefing are fundamental to the intelligence profession.



Major, James S. *Communicating with Intelligence*. Lanham, MD: Rowman & Littlefield, 2014.

40

****040** So even if you've done great analysis, yet you're unable to communicate your findings or your assessments clearly and effectively, it's really not going to matter.

Intelligence Writing – Some Tips

- Focuses on the future
- Written for generalists facing real problems
- Act of meaningful Characterization
- Begins with bottom line then explores their implication
- Anything more than 5 pages on one particular topic or event, may not be read by many people.



James S. Major, *Communicating with Intelligence*.
Second Edition. London. 2014.. Rowman and Littlefield.

41

**041 Intelligence writing often, but not always, focuses on the future, and many intelligence reports try to focus on the future and judge what might happen or what will happen in the future. For example, "We judge Russia will launch more sophisticated cyberattacks against Ukraine," or "We judge that ransomware will continue to be the tactic of choice for ABC Organized Crime Group."

When you're in a more operationally fast-paced type environment, doing intelligence assessments on the future is a big challenging because you're typically just trying to keep up and assess what is going on in any particular situation and make recommendations and provide deeper insight and context for operators in the field. At the very least though, you should be trying to provide

operators in the field with new insight and meaning.

Intelligence writing tends to be written for generalists facing real problems. So intel analysts, when they go and brief and write, they are usually doing that for people that are generalists, policymakers, decision-makers, that do not have the same depth of knowledge as the technical folks do. So the products should be written and briefed in a manner that is comprehensible for a generalist, the idea of being able to communicate technical language into nontechnical language for nontechnical audiences at different altitudes within an organization is-- and I think personally will be very much needed in the future for people going into this field.

The notion of Act of Meaningful Characterization means that you should go beyond just listing facts and attempting to draw conclusions from facts. That's what the Act of Meaningful Characterization means. It means don't just list facts, try to add some context. It is basically doing analysis, correlations, using multiple sources of intelligence, using analytical methods. Again, don't just list facts, because anyone can do that. Your job is to make them meaningful, relevant, and provide insight that goes beyond just fact-listing.

Begin with the bottom line and then explore their implication. Can't stress that enough. Always start with the

bottom line, explore your implication, and then anything more than five pages on one particular topic or event may not be read by many people.

Know your Audience

Know your Audience

- Who will be reading your product, or who will you be briefing to?
- How much does your audience already know about the subject?
- Why does your audience care?
- How will your audience use / or would you like for them use the information you give them?

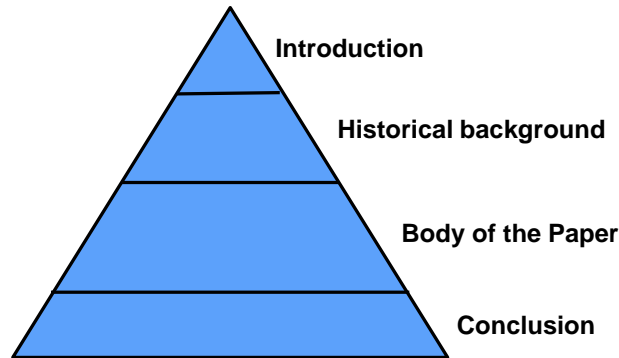


42

****042** Before you begin to write, you must ask your these questions before you begin. Who will be reading your product or who will you be briefing to? How much does your audience already know about the subject? Why does your audience care? How will or how would you like for them to use the information that you're going to give them? You should be thinking about these things before you write and while you are writing, and also don't forget to figure out when the product is due.

Intelligence Writing Is Not Academic Writing -1

- **Academic Writing** – Logical flow is usually researcher's evidence in increasing order of significance and builds to a closing conclusion.



Critical Thinking for Intelligence. Katherine Hibbs Pherson, Randolph H. Pherson. Sage Publications 2013.

43

**043 Intelligence writing is not academic writing. Academic writing was what I was taught when I was in high school or college. Academic writing usually goes like this: First you have an introduction. In the introduction you talk about what the paper is going to be about, why you're writing about this particular topic, how the paper is organized. So, "The first part of the paper will talk about this, the second part will talk about that, the third part," etcetera, etcetera. You also have the research methodology, how you went about doing your research, and the timeframe for the research. The next section typically goes into some historical background where you have the history of a prior assessment on the research topic. Then you're going to get into the body of the paper, where you're

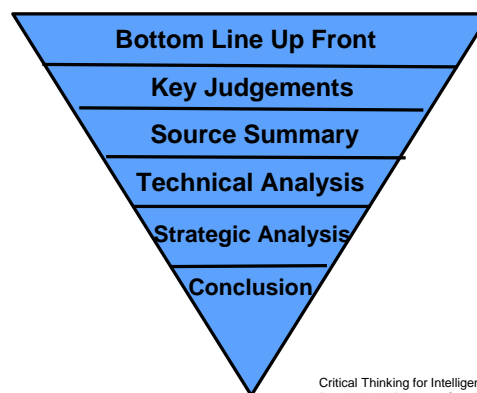
diving into details, and then you have your conclusion where you wrap up everything in a nice summary. So that is actually the opposite way of how you should do intelligence writing. Don't do that when you're writing intelligence as a cyber intelligence analyst.

Intelligence Writing Is Not Academic Writing -2

Intelligence Writing Is Not Academic Writing -2

Intelligence Writing starts with the most important concept and has reasoning and analysis that follows.

Order Typically Follows:



Critical Thinking for Intelligence. Katherine Hibbs Pherson, Randolph H. Pherson. Sage Publications 2013.

44

****044** What you want to do is something like this. This is generally the conceptual order or framework for intelligence writing. Intelligence writing is the opposite way from academic writing largely because decision-makers do not have time to read your entire paper to get to your conclusions. They want to know right up front what they need to know. So certain intelligent organizations, bosses, companies or agencies, they may differ in the exact order or even naming convention on

this slide and these sections that I'm about to talk about, but all of them are going to tell you to keep the Bottom Line Up Front, followed by Key Judgments. So let's talk about these more in-depth.

So you have your Bottom Line Up Front, and sometimes that's called a BLUF. This is your main point or recommendation or idea that you want to get across to a decision-maker. Next is your Key Judgments about your topic. These are typically statements that begin with the words, "We judge" or "We assess" or "We estimate with low or moderate confidence that ABC country will launch a cyberattack against XYZ country."

Next is your Source Summary, and that is a summary about the sources you have used to support you and where you get your information, and then the next could be Technical Threat Analysis, followed by your Strategic Analysis, depending on the issue you're working on. This is the more technical aspect, and then the strategic is where you're focusing on the broader impact to your organization or industry. And then the conclusion is the last section, and while this is more or less just a restatement of your Bottom Line Up Front, it should always have more context than your Bottom Line Up Front, and I'll talk about that in the next few minutes. But let's go deeper into these sections.

Bottom-Line-Up-Front (BLUF)

- Do not start a paper by defining methods or purpose of the paper.

Ex of what NOT to do: *This paper will look at key influential and rising hackers. First, this study will attempt to show the possible reasons why these particular hackers are gaining influence. Following that, the paper will explore all the skills and capabilities of these hackers. Finally, the paper will conclude with a forecast for which particular hackers will become the senior leaders.*

- Get right to the point.
 - Answer the question what your reader wants to know in the first paragraph.



45

****045 So Bottom Line Up Front.**

Don't start a paper by defining the methodology in which you did your analysis or the purpose of your paper. In other words, here's an example of what not to do. Don't do something that says, "This paper will look at key influential and rising hackers. First this study will attempt to show the possible reasons why these hackers are gaining influence. Following that the paper is going to talk about the skills and the capabilities of the hackers, and finally the paper will conclude about which particular hackers will become senior leaders."

Don't do that. What you really want to do is get right to the point with your Bottom Line Up Front. You want to answer the main question that leadership has, because leadership-- they don't have the time to know all the methods that you used. They want to know what the

bottom line is. If they have additional questions about your Bottom Line Up Front, they can always ask you and you can give them the information that they need. So you want to get right to the point; answer the question that your reader wants to know in the first paragraph.

BLUF 1st Paragraph Tips

BLUF 1st Paragraph Tips

- Do not exceed five sentences.
- State your assessment using estimative language.
- Make it a summary of the key points made throughout the analytical product.
- Briefly answer who, what, where, when, why, and how.
- Then, expand on the information in the analysis sections.
- Provide recommendations.
- Write it last in BLUF.



46

**046 So for your BLUF, that typically should be one paragraph. It should not exceed five sentences. You should state your assessment using estimative language. It should be a summary of the key points you made throughout your analytical product, and if you can-- and this is not saying you have to do this; these are things you should attempt to do if possible when you're writing your BLUF-- you should try to answer who, what, when, where, and why and how the particular issue you're

looking at, and I would always recommend writing the BLUF last when you're doing your assessment.

Key Judgements

Key Judgements

- Must convey accurately and succinctly the analytical findings of the paper
- Exclude source information used in the paper, persons consulted during preparation, or analytical methodologies
- Generally should not exceed 10% of your paper
- Are in bullet format, listed in order of importance
- Example

"We judge with high confidence that in fall 2003, Tehran halted its nuclear weapons program; we also assess with moderate-to-high confidence that Tehran at a minimum is keeping open the option to develop nuclear weapons."



James S. Major. Communicating with Intelligence. Second Edition. London. 2014.. Rowman and Littlefield.
November 2007 National Intelligence Estimate, "Iran: Nuclear Intentions and Capabilities"

48

****048** Key Judgments are usually read by leadership. They must convey accurately and succinctly the analytical findings of the paper. Key Judgments should not include source of information that you use, persons consulted during preparation, or who you coordinated with, or analytical methodologies employed. Key Judgments convey what the analyst would say or should say to a high-level decision-maker if given only two minutes in which to convey the findings.

So here's an example of a Key Judgment from a November 2007 National Intelligence Estimate about Iran's nuclear intentions and

capabilities as classified and released by the Office of Director of National Intelligence. The example is, "We judge with high confidence that in the fall of 2003 Tehran halted its nuclear weapons program. We also assess with moderate to high confidence that Iran at a minimum is keeping open the option to develop nuclear weapons." So that's an example of a Key Judgment.

Source Summary Statement

Source Summary Statement

- 1 - 2 paragraphs – **(Preferably one)** Paras should not exceed five - six sentences.
- Focus on types of sources, credibility, reliability, date of information, and relevance to the intelligence provided.
- Example

"Analytical findings are based on multi-source intelligence reporting over the last two years. SIGINT detailing XYZ threat actor capabilities was corroborated with two long-time HUMINT sources assessed to be reliable and whose reporting on past and different cyber threat actors has been corroborated. OSINT (pastebin / IRC, dark web chats) often corroborated classified reporting yet we are unable to fully determine the reliability and credibility of those OSINT sources on such platforms."



49

****049** So your Source Summary statement should be one or two paragraphs, preferably one. Paragraphs should, again, not try to exceed five or six sentences. And this section is where you try to speak to the types of sources you used, the credibility, reliability and relevance of the intelligence provided. Additionally, you should have footnotes or endnotes, depending on

your particular employer's preference. I think it would also be a good idea to place or note where your intel gaps are, although I've seen some reports where intelligence gaps are at the end of the assessment, and here's an example of a Source Summary statement that I just made up. "Analytical findings are based on multi-source intelligence reporting over the last two years. SIGINT dealing with XYZ threat actors was corroborated with two long-time HUMINT sources assessed to be reliable and whose reporting on past and different cyber threat actors has been corroborated. OSINT often corroborated classified reporting yet we are unable to fully determine the reliability and credibility of those OSINT sources on the platform."

Intelligence Gaps

- Write them as statements, not questions.
 - In the statements, identify:
 - The intelligence gap
 - Why it is a gap for your assessment
 - What is needed to fill the gap
 - Example

"This assessment lacks insight into phone and encrypted chat communications. We consider this a gap in our assessment because understanding communications could provide us with clarity regarding TTP modifications and possible next targets. Recommend focusing SIGINT collection platforms for this purpose."



50

****050** In terms of intelligence gaps, write them as statements, not questions. In the statements identify the specific intelligence gap, why it is a gap per your assessment, what is needed to fill the gap. An example could be, "This assessment lacks insight into phone and encrypted chat communication. We consider this a gap in our assessment because understanding actor communications could provide us with clarity regarding TTP modifications and possible next targets. Recommend focusing SIGINT collection patterns for this purpose." So that's an example of stating intelligence gaps.

Threat and Strategic Analysis

- Circa 1 to 2 paragraphs for Threat and Strategic Analysis Each
- Employ the decreasing importance style; avoid increasing
- Start with the most recent info, then work your way back in time
- Inform about what, if any, analytical methodologies used during your analysis that aided in forming your judgments
- Threat Analysis (Technical) – What, How, When, Where
- Strategic Analysis (Holistic) – Rooted in Threat Analysis yet focuses on Who and Why (threats) / or other topics geopolitics, emerging technology



51

**051 Threat and Strategic Analysis.

So obviously if you're a political intelligence analyst or counterintelligence analyst or denial or deception analyst, you may not have a technical portion or your technical portion may be different than a cyber intelligence analyst, and that is totally fine; you got to do what makes sense. However, for our purposes, as a cyber intelligence analyst, you should have a Technical Threat and Strategic Analysis section. Each section should be one to two paragraphs long. However, there is really no hard and fast rule about that. I am a big fan of brevity, so the shorter the better in my opinion.

Your analysis should also employ decreasing importance of style, meaning start with the most important parts of your analysis and

work back in decreasing order of importance. Think of your Technical Analysis section as your Threat Analysis section, which should address the what, how, where, and when questions of your cyber issue. Think of your Strategic Assessment as addressing the who and the why when it comes to particular threat actors, or a deep analysis on trends in the industry about a particular topic or technology. In these sections, you should also inform about what analytical methods, if any, were employed to assist your analysis that help with your judgments.

Conclusion

Conclusion

- Make sure the reader walks away with what they need.
 - **Unique** – Flows organically from everything that came before it
 - **Substantive** – Has meaning, gives the reader something to consider, more context than BLUF
 - **Proportional** – Length of conclusion depends on length and complexity of paper
 - **Consistent** – Should convey the same overall message in the BLUF; consistent in tone and attitude of rest of paper
 - **Not a copy and paste of BLUF**
- Do not leave any cliffhangers.



James S. Major and Dianan Raschke, *Communicating with Intelligence*, Second Edition. London, 2014. Rowman and Littlefield.

52

****052** Whether you write a conclusion is honestly a judgment call based on your company, organization, and you, your role, responsibilities, and how much time

you actually have. In some cases, if you only have a page or a page and a half of text, you probably do not need to write a conclusion. If you do have a conclusion, you want to make sure the reader walks away with what they need to know. So think of your conclusion as your last chance to convey your meaning to the audience or the reader, and because of that, you really want a strong conclusion. Since the consumer of your product has already reached the conclusion, meaning that they've read through the entire paper, feel free to synthesize your analysis a bit more with more detail or in a way that best captures your meaning and what you want your reader to remember and act on at the end. So like the BLUF, the conclusion brings all the pieces together, but in the conclusion you have more flexibility to allude to people, places, concepts, attacks covered earlier in the paper.

Here's some tips for your conclusion. Try to make it unique, meaning it should flow organically from everything that came before it. Substantive-- it should have meaning and gives a reader something to consider. It should be proportional, meaning that the length of the conclusion depends on the length and complexity of your paper. Your conclusion should not be three paragraphs if your paper is two paragraphs long. It should also be consistent, meaning that it should convey the same overall message in the BLUF, consistent in tone and attitude with the rest of the paper.

There should be no mixed messages,
and the conclusion should not just be
a copy-and-paste of your BLUF.

Intelligence Writing Tips -1

Intelligence Writing Tips -1

- Align **Threat / Strategic** analytical paragraphs with this format.
 - Topic sentence: Convey the most important idea/information.
 - Use 2-3 detailed sentences to expand/provide more context on the topic sentence.
 - Last sentence: Reemphasize the paragraph's main point and/or transition to next paragraph or section.
 - Paragraphs should be 4-5 sentences. **Never longer than six sentences.**
- Revise, revise, revise.
- Use active, not passive voice.
 - Subject – verb – object
 - If not, we'll be asking a lot of "whodunit" questions.



54

****054** Here's some overall intelligence writing tips. First, you want to align the Threat and Strategic analytical paragraphs with this format. You should have a topic sentence, which conveys the most important idea or information for the paragraph. Then you should have two to three detailed sentences to expand or provide more context about that particular topic sentence, and then you wrap it up with the last sentence, which reemphasizes the paragraph's main point, or you're transitioning to your next paragraph or section. Again, paragraphs should be four to five sentences long, not longer than six sentences. You also want to try to use active voice. So,

for example, "The cyberattack destroyed the server," is the active voice. The passive voice would be, "The server was destroyed by the cyberattack." You want to use the active voice.

Intelligence Writing Tips -2

Intelligence Writing Tips -2

- Be clear – One person's 'simple' is another person's 'huh?'
 - Use footnotes to explain concepts, terms, methods, etc.
- Be concise – Use as few words as possible.
- Be precise – Say exactly what you mean.
- Use strong verbs.
- Print the product and read it out loud.
- Spend time prewriting.
- There is no magic formula for being a good writer – have grit!



55

****055** Some more intelligence writing tips. Be clear. Simple words are always better. There's no need to try to use fancy GRE words or jargon. Those words are typically viewed as anathema to your colleagues in general. There's some irony there. But footnotes are great also, especially in the cyber domain, and always remember that words mean different things to different people, such as the words "potential" or "possible" or "likely". And then always try to be concise. Less is generally more.

Intelligence Writing Tips -3

- Wikipedia's Neutral Point of View
 - Avoid stating opinions as facts.
 - Avoid stating seriously contested assertions as facts.
 - Avoiding stating facts as opinions.
 - Indicate the relative prominence of opposing view.



https://en.wikipedia.org/wiki/Wikipedia:Neutral_point_of_view

56

****056** Here's some additional tips.

Avoid stating opinions as facts. Avoid stating seriously contested assertions as facts. Avoid stating facts as opinions. And indicate the relative prominence of opposing views.

Notices

Notices

Copyright 2020 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

CERT® is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM20-0262

